UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ERIN WEILER individually and on behalf of all others similarly situated, Plaintiff, v. WUNDERKIND CORPORATION, Defendant.	Case No: 25-5854 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Dated: July 16, 2025

BURSOR & FISHER, P.A.
Philip L. Fraietta
Yizchak Kopel
Alec M. Leslie
Max S. Roberts
Victoria X. Zhou
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
ykopel@bursor.com
aleslie@bursor.com
mroberts@bursor.com
vzhou@bursor.com

Attorneys for Plaintiff

TABLE OF CONTENTS

PAGE

Plaintiff Erin Weiler ("Plaintiff") brings this action on behalf of herself and all others similarly situated against Defendant Wunderkind Corporation ("Defendant"). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations pertaining to herself, which are based on personal knowledge.

NATURE OF THE ACTION

1. This class action lawsuit sets forth how the business practices of Defendant amounts to a deliberate surveillance of millions of Americans through their activity on the Internet and mobile applications. Wunderkind, through its software products, tracks in real time and records indefinitely the personal information and specific web activity of hundreds of millions of Americans.

2. This unlawfully collected information is worth billions of dollars to Defendant because it makes up the content of Defendant's Identity Network and creates individual sales of advertisements in the real-time-bidding ecosystem present on thousands of major websites where Defendant's services are installed.

3. Plaintiff, like other Class Members, was the victim of Defendant's widespread privacy surveillance, as she was tracked ***over 45,000 times*** by Defendant according to her CCPA data.

4. Plaintiff brings this action to enforce her constitutional rights to privacy and to seek damages under Federal law for the harm caused by the collection and sale of her confidential data and personal information.

THE PARTIES

5. Plaintiff Erin Weiler is a natural person and citizen of California, residing in Los Angeles, California. Plaintiff Weiler was in California when she accessed the E! Online website

(among others) and had her activity on that website and subsequent activity on other websites tracked by Defendant.

6. Defendant Wunderkind Corporation is a Delaware corporation with its principal place of business at 1 World Trade Center, Floor 74, New York, New York 10007. Wunderkind is a data broker that adds the IP addresses and Device Metadata of Website users to comprehensive user profiles and uses that information to track Plaintiff and Class Members across the Internet. Those data profiles are then provided to advertisers for more targeted and tailored advertising based on a broad universe of information.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

8. This Court has personal jurisdiction over Defendant because Defendant is domiciled in this District.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is domiciled in this District.

FACTUAL ALLEGATIONS

I. DATA BROKERS AND REAL-TIME BIDDING: THE INFORMATION ECONOMY

10. To put the invasiveness of Defendant's privacy violations into perspective, it is important to understand three concepts: data brokers, real-time bidding, and cookie syncing.

11. In short, the import of these concepts is that: (i) Defendant is a data broker that collects user information from website visitors to uniquely identify and de-anonymize users and

compile their information into a comprehensive profile; (ii) Defendant shares those profiles with various third party Partner Pixels (through cookie syncing); and (iii) those profiles are offered up for sale through the real-time bidding process to the benefit of Defendant's clients and to the detriment of users' privacy interests.

A. Data Brokers

12. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"[1] the Federal Trade Commission defines "data broker[s]" as "companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies."[2]

13. Any entity that qualifies as a "data broker" under California law must specifically register as such (Cal. Civ. Code § 1798.99.82(a)), which Wunderkind does.[3]

14. Some data brokers prefer to characterize themselves as "identity graph providers," but this is a distinction without a difference. "An identity graph provides a single unified view of customers and prospects based on their interactions with a product or website across a set of devices and identifiers. An identity graph is used for real-time personalization and advertising targeting for millions of users."[4] This is exactly what data brokers do, and indeed, the entities that

[1] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, DUKE SANFORD CYBER POLICY PROGRAM, at 2 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

[2] *FTC to Study Data Broker Industry's Collection and Use of Consumer Data*, FTC, https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data (last visited June 3, 2025).

[3] DATA BROKER REGISTRATION FOR WUNDERKIND CORPORATION, https://oag.ca.gov/data-broker/registration/191359.

[4] IDENTITY GRAPHS ON AWS, https://aws.amazon.com/neptune/identity-graphs-on-aws/.

provide identity graphs are by and large required to register as data brokers under California law. An "identity graph provider" is therefore just a euphemism for "data broker."

15. "Data brokers typically offer pre-packaged databases of information to potential buyers," either through the "outright s[ale of] data on individuals" or by "licens[ing] and otherwise shar[ing] the data with third parties."[5] Such databases are extensive, and can "not only include information publicly available [such as] from Facebook but also the user's exact residential address, date and year of birth, and political affiliation," in addition to "inferences [that] can be made from the combined data." And whereas individual data sources "may provide only a few elements about a person's activities, data brokers combine these elements to form a detailed, composite view of the consumer's life."[6]

16. For instance, as a report by NATO found, data brokers, like Defendant, collect two sets of information: "observed and inferred (or modelled)." The former "is data that has been collected and is actual," such as websites visited.[7] Inferred data "is gleaned from observed data by modelling or profiling," meaning what consumers may be *expected* to do.[8] On top of this, "[b]rokers typically collect not only what they immediately need or can use, but hoover up as much information as possible to compile comprehensive data sets that might have some future use."[9]

---

[5] Sherman, *supra*, at 2 (2021).

[6] Tehila Minkus et al., *The City Privacy Attack: Social Media and Public Records for Detailed Profiles of Adults and Children*, COSN '15: PROCEEDINGS OF THE 2015 ACM CONFERENCE ON ONLINE SOCIAL NETWORKS, at 71, (2015), https://dl.acm.org/doi/pdf/10.1145/2817946.2817957.

[7] Henrik Twetman & Gundars Bergmanis-Korats, *Data Brokers and Security*, at 11, NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[8] *Id*.

[9] *Id*.

17. Likewise, a report by the Duke Sanford Cyber Policy Program "examine[d] 10 major data brokers and the highly sensitive data they hold on U.S. individuals."[10] The report found that "data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees."[11]

18. This data collection has grave implications for Americans' right to privacy. For instance, "U.S. federal agencies from the Federal Bureau of Investigation [] to U.S. Immigration and Customs Enforcement [] purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations."[12]

19. As another example:

> Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals' civil rights. Even if data brokers do not explicitly advertise these types of data (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make "predictions" or "inferences" about this kind of sensitive information (race, gender, sexual orientation, etc.) on individuals.
>
> This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements. Many

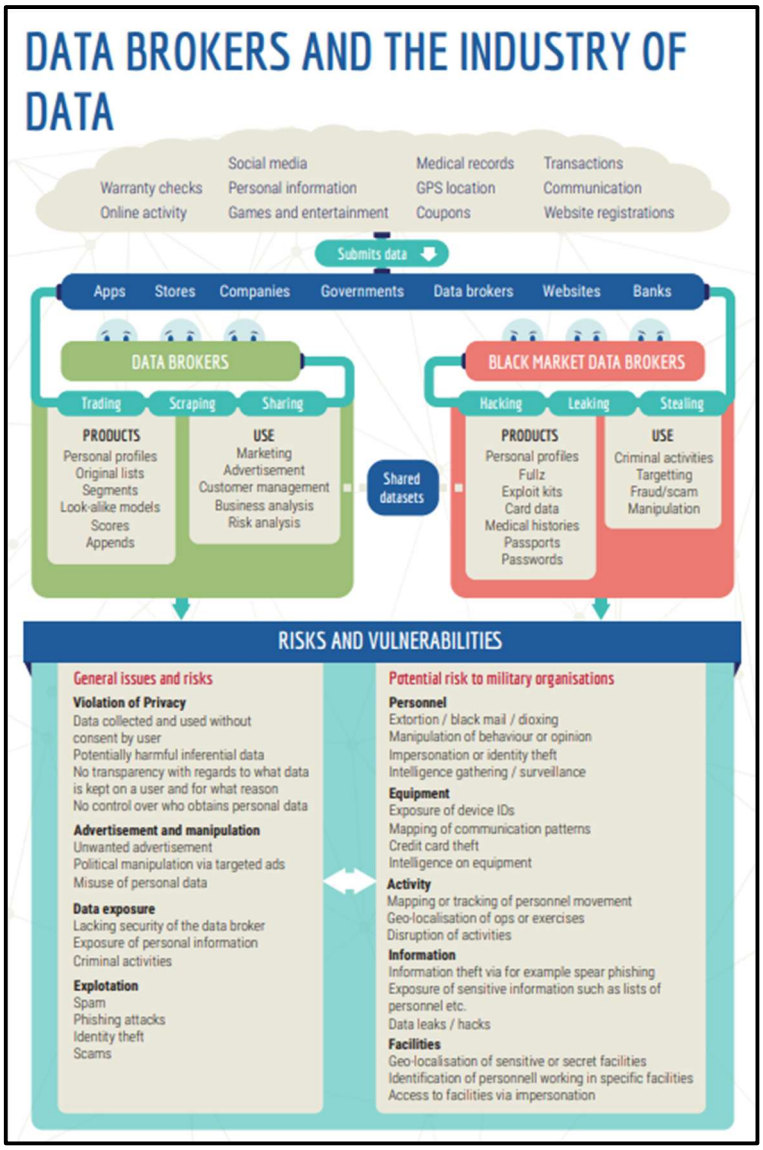
[10] Sherman, *supra*, at 1.

[11] *Id*.

[12] *Id*. at 9.

> industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services.
>
> …
>
> Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups.

20. Similarly, as the report from NATO noted, corporate data brokers cause numerous privacy harms, including but not limited to depriving consumers of the right to control who does



and does not acquire their personal information, unwanted advertisements that can even go as far as manipulating viewpoints, and spam and phishing attacks.[13]

21. In the modern age, these threats are far too real. For instance, the gunman who assassinated a Minnesota state representative and her husband "may have gotten their addresses or other personal details from online data broker services, according to court documents."[14] Similarly, following the protests in Los Angeles:

> Tech-skeptical California lawmakers and activists fear the Trump administration will leverage tech tools to track and punish demonstrators accused of interfering with Immigration and Customs Enforcement raids. One possible instrument at ICE's disposal: location data, a highly detailed record of people's daily movements that's collected and sold by everything from weather apps to data brokers.[15]

22. Data brokers like Defendant are able to compile such wide swaths of information in part by collecting users' IP addresses and other device information, which is used by data brokers like Defendant to track users across the Internet.[16] Indeed, as McAfee (a data security company) notes, "data brokers … can even place trackers or cookies on your browsers … [that] track your IP address and browsing history, which third parties can exploit."[17] These data brokers will then:

---

[13] Twetman & Bergmanis-Korats, *supra* note 9, at 8.

[14] Lily Hay Newman, *Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets' Addresses*, WIRED (June 16, 2025), https://www.wired.com/story/minnesota-lawmaker-shootings-people-search-data-brokers/.

[15] Tyler Katzenberger, *LA Protests Fuel California Drive To Hide Data From Trump*, POLITICO (June 11, 2025), https://www.politico.com/news/2025/06/11/la-protests-california-hide-data-trump-00400127

[16] *Id*. at 11.

[17] Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, MCAFEE (Jan. 28, 2025), https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/.

> take that data and pair it with other data they've collected about you, pool it together with other data they've got on you, and then share all of it with businesses who want to market to you. They can eventually build large datasets about you with things like: "browsed gym shorts, vegan, living in Los Angeles, income between $65k-90k, traveler, and single." Then, they sort you into groups of other people like you, so they can sell those lists of like-people and generate their income.[18]

23. In short, data brokers like Defendant track consumers across the Internet, compiling various bits of information about users, building comprehensive user profiles that include an assortment of information, interests, and inferences, and offering up that information for sale to the highest bidder. The "highest bidder" is a literal term, as explained below.

B. Real-Time Bidding

24. So, once data brokers like Defendant collect information from consumers and create comprehensive user profiles, how does Defendant "sell" or otherwise monetize that information? This is where real-time bidding comes in.

25. "Real Time Bidding (RTB) is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application."[19]

26. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)."[20] An SSP "work[s] with website or app publishers to help them participate in the RTB process."[21] "DSPs

---

[18] Paul Jarvis, *The Problem with Data Brokers: Targeted Ads and Your Privacy*, FATHOM ANALYTICS (May 10, 2022), https://usefathom.com/blog/data-brokers.

[19] Sara Geoghegan, *What is Real Time Bidding?,* ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.

[20] *Id*.

[21] *Id*.

primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth."[22] And an Advertising Exchange "allow[s] advertisers and publishers to buy and sell ad inventory directly through real time bidding, and without the need to have an intermediary involved in the transaction. This model offers several benefits for advertisers and publishers including transparency, flexibility, and a greater degree of control over their inventory."[23]

27. In other words, SSPs provide user information to advertisers that might be interested in those users, DSPs help advertisers select which users to advertise and target, and an Advertising Exchange is the platform on which all of this happens.

28. The RTB process works as follows:

> After a user loads a website or app, an SSP will send user data to Advertising Exchanges … The user data, often referred to as "bidstream data," contains information like device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an Advertising Exchange will broadcast the data to several DSPs. The DSPs will then examine the broadcasted data to determine whether to make a bid on behalf of their client.
>
> Ultimately, if the DSP wins the bid, its client's advertisement will appear to the user. Since most RTB auctions are held on the server/exchange side, instead of the client/browser side, the user only actually sees the winner of the auction and would not be aware of the DSPs who bid and lost. But even the losing DSPs still benefit because they also receive and collect the user data broadcasted during the RTB auction process. This information can be added to existing dossiers DSPs have on a user.[24]

---

[22] *Id.*

[23] Brock Munro, *What is an Ad Exchange and How Does It Work*, PUBLIFT (Feb. 28, 2025), https://www.publift.com/blog/what-is-an-ad-exchange.

[24] Geoghegan, *supra*; *see also Real-Time Bidding*, APPSFLYER, https://www.appsflyer.com/glossary/real-time-bidding/ (last visited June 3, 2025).

29. Facilitating this real-time bidding process means SSPs and DSPs must have as much information as possible about a website's users to procure the greatest interest from advertisers and the highest bids. These entities receive assistance because various websites also install the trackers of data brokers like Defendant on their users' browsers:

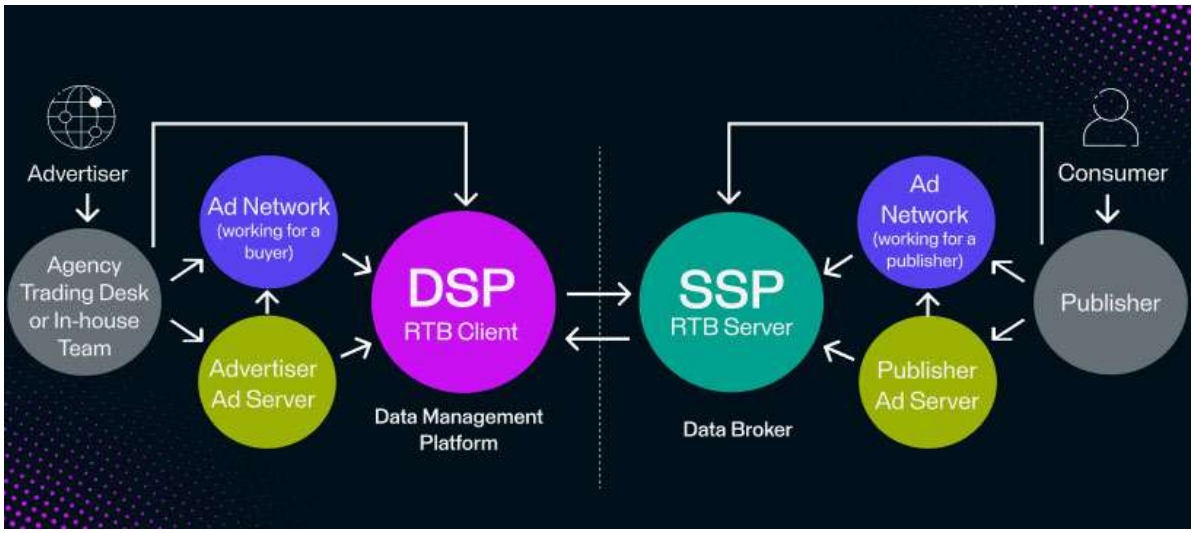
> the economic incentives of an auction mean that DSP [or SSP] with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP enlists a final actor, the data management platform (DMP) [or a data broker]. DSPs [or SSPs] send bid requests to DMPs [and data brokers], who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser, collected from other sources, or bought from data brokers. The DSP with the highest bid not only wins the right to deliver the ad—through the SSP—to the individual. The DSP also wins the right to cookie sync its own cookies with those from the [Advertising Exchange], thus enabling easier linkage of the data to the user's profile in the future.[25]

//

//

//

[25] Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226, 232-33 (2022), https://tinyurl.com/yjddt5ey.



30. In other words, SSPs can solicit the highest bids for website users by identifying and de-anonymizing those users by combining the information they collect directly from website users with the information other data brokers like Defendant know about that user. If there is a match, then these data brokers will have significantly more information to provide about users, and that will solicit significantly higher bids from prospective advertisers (because the advertisers will have more information about the user to target their bids).

31. Likewise, a DSP can generate the highest and most targeted bids from advertisers with providing those advertisers with as much information about users as possible, which they do by syncing with the trackers of data brokers like Defendant.

32. All this naturally enriches website operators, as its users have now become more valuable thanks to the replete information data brokers like Defendant are able to provide about users. And Defendant benefits too, as it increases the vast array of information it knows about users, making

33. As the Federal Trade Commission ("FTC") has noted, "[t]he use of real-time bidding presents potential concerns," including but not limited to:

(i) "incentiviz[ing] invasive data-sharing" by "push[ing] publishers [*i.e.*, website and app operators] to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior."

(ii) "send[ing] sensitive data across geographic borders."

(iii) sending consumer data "to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways."[26]

34. The last point bears additional emphasis, as it means the data Defendant provides to DSPs to serve targeted advertisements is even provided to those entities who do not actually serve an advertisement on a consumer. This greatly diminishes the ability of users to control their personal information.

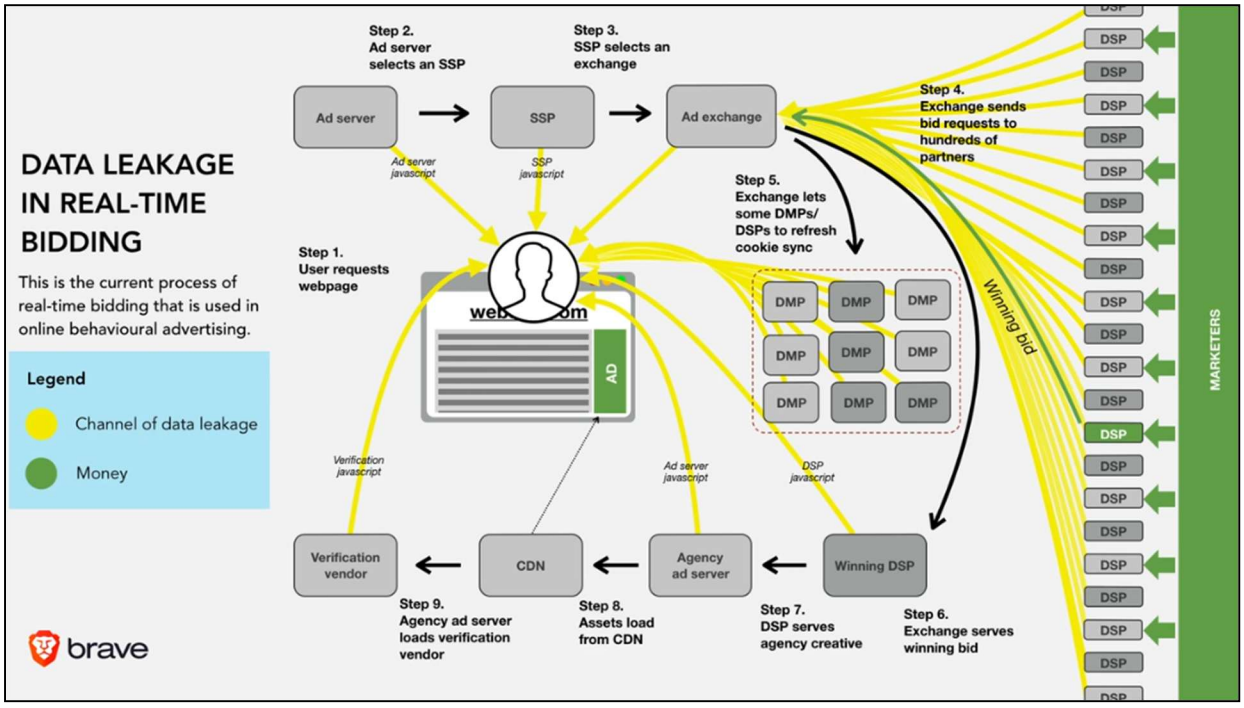
35. Likewise, the Electronic Privacy Information Center ("EPIC") has warned that "[c]onsumers' privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations."[27]

36. For these reasons, some have characterized "real-time bidding" as "[t]he biggest data breach ever recorded" because of the sheer number of entities that receive personal information[28]:

[26] *Unpacking Real Time Bidding through FTC's case on Mobilewalla*, FEDERAL TRADE COMMISSION, (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

[27] Geoghegan, *supra*.

[28] Dr. Johnny Ryan, "RTB" ADTECH & GDPR, https://assortedmaterials.com/rtb-evidence/ (last visited June 3, 2025).



37. All of this is in line with protecting the right to determine who does and does not get to know one's information, a harm long recognized at common law and one the California Invasion of Privacy Act and other wiretapping statutes were enacted to protect against. *Ribas v. Clark*, 38 Cal. 3d 355, 361 (1985) (noting the CIPA was drafted with a two-party consent requirement to protect "the right to control the nature and extent of the firsthand dissemination of [one's] statements"); *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763-64 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

C. Cookie Syncing

38. It should now be clear both the capabilities of Defendant (*i.e.*, a data broker who de-anonymizes users) and the reasons website operators use Defendant's on their websites (to sell user information to advertisers in real-time bidding by identifying users and providing advertisers with as much information about users as possible to solicit the highest bids). The final question is

how does Defendant share information with others to offer these complete user profiles up for sale? This occurs through "cookie syncing."

39. Cookie syncing is a process that "allow[s] web companies to share (synchronize) cookies and match the different IDs they assign for the same user while they browse the web."[29] This allows entities like the Third Parties to circumvent "the restriction that sites can't read each other cookies, in order to better facilitate targeting and real-time bidding."[30]

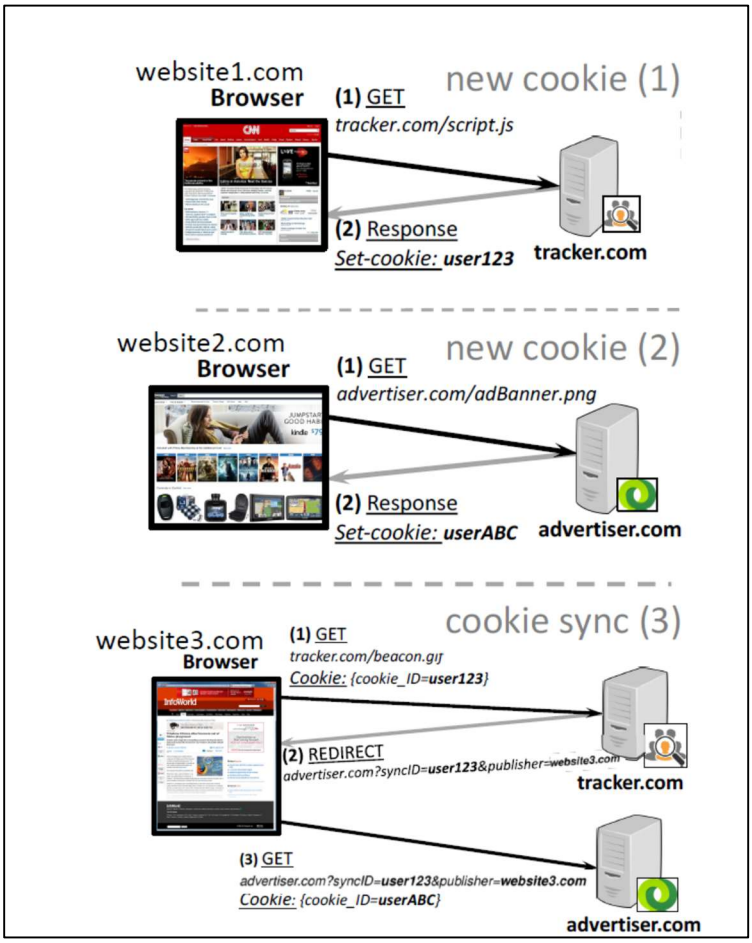
40. Cookie syncing works as follows:

> Let us assume a user browsing several domains like website1.com and website2.com, in which there are 3rd-parties like tracker.com and advertiser.com, respectively. Consequently, these two 3rd-parties have the chance to set their own cookies on the user's browser, in order to re-identify the user in the future. Hence, tracker.com knows the user with the ID user123, and advertiser.com knows the same user with the ID userABC.
>
> Now let us assume that the user lands on a website (say website3.com), which includes some JavaScript code from tracker.com but not from advertiser.com. Thus, advertiser.com does not (and cannot) know which users visit website3.com. However, *as soon as the code of tracker.com is called, a GET request is issued by the browser to tracker.com (step 1), and it responds back with a REDIRECT request (step 2), instructing the user's browser to issue another GET request to its collaborator advertiser.com this time, using a specifically crafted URL (step 3)*.
>
> …
>
> When advertiser.com receives the above request along with the cookie ID userABC, it finds out that userABC visited website3.com. *To make matters worse, advertiser.com also learns that the user whom tracker.com knows as user123, and the*

[29] Panagiotis Papadopoulos et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, 1 WWW '19: THE WORLD WIDE WEB CONFERENCE 1432, 1432 (2019), https://dl.acm.org/doi/10.1145/3308558.3313542.

[30] Gunes Acar et al., *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, 6B CCS'14: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 674, 674 (2014)

user userABC is basically one and the same user. Effectively, CSync enabled advertiser.com to collaborate with tracker.com, in order to: (i) find out which users visit website3.com, and (ii) *synchronize (i.e., join) two different identities (cookies) of the same user on the web*.[31]



41. Through this process, third party trackers are not only able to resolve user identities (*e.g.*, learning that who Third Party #1 knew as "userABC" and Third Party #2 knew as "user123" are the same person), they can "track a user to a much larger number of websites," even though that "do not have any collaboration with" the third party.[32]

[31] Papadopoulos, *supra*, at 1433 (emphasis added).

[32] Papadopoulos, *supra*, at 1434.

42. On the flip side, "CSync may re-identify web users even after they delete their cookies."[33] "[W]hen a user erases her browser state and restarts browsing, trackers usually place and sync a new set of userIDs, and eventually reconstruct a new browsing history."[34] But if a tracker can "respawn" its cookie or like to another persistent identifier (like an IP address), "then through CSync, all of them can link the user's browsing histories from before and after her state erasure. Consequently: (i) users are not able to abolish their assigned userIDs even after carefully erasing their set cookies, and (ii) trackers are enabled to link user's history across state resets."[35]

43. Thus, "syncing userIDs of a given user increases the user identifiability while browsing, thus reducing their overall anonymity on the Web."[36]

44. Cookie syncing is precisely what is happening here. When Defendant's tracker is installed on website users' browsers, it syncs with other third parties on the website. The result of this process is not only that a single user is identified as one person by these multiple third parties, but they share all the information about that user with one another. This prevents users from being anonymous when they visit websites where Defendant's tracker is installed.

* * *

45. To summarize the proceeding allegations, Defendant is a data broker that focuses on collecting as much information about users as possible to create comprehensive user profiles. Defendant may collect IP Addresses, Device Metadata, and unique user IDs in the first instance, but those pieces of information are connected to information Defendant glean from other sources (*e.g.*, various data brokers) to build comprehensive profiles. Through "cookie syncing," those

[33] *Id.*

[34] *See id.*

[35] *Id.*

[36] *Id.* at 1441.

profiles are shared with other entities to form the most fulsome picture with the most attributes as possible. And those profiles are offered up for sale to advertisers through real-time bidding, where users will command more value the more advertisers know about a user.

46. Thus, partnering with Defendant allows website operates to enrich the value users' information would otherwise command by tying the data Defendant obtains directly from users on websites (*e.g.*, IP addresses, Device Metadata, unique user IDs) with comprehensive user profiles.

47. Defendant benefits from this arrangement as well because websites and apps will want to employ Defendant's services to bring in more advertising revenue, meaning Defendant can continue to expand and grow the information it has about any consumers and add to consumers' profiles, which further perpetuates the value of Defendant's services.

48. Defendant is already one of the largest players in this industry. Defendant achieved this status through the use of a variety of technologies and services, as described below.

II. DEFENDANT COLLECTS PLAINTIFF'S AND CLASS MEMBERS' PERSONAL INFORMATION ON WEBSITES WHERE ITS TRACKERS ARE PRESENT

49. One way Defendant tracks individuals across multiple websites is through the use of persistent identifiers. As the name suggests, persistent identifiers identify information that follows an Internet user from one website or app to another. Defendant uses these identifiers to confirm that using a particular website is the same person identified by Defendant on another website (or on another visit to the same website).

A. E-mail Addresses

50. Most prominently, Defendant collects e-mail addresses through its trackers.[37]

[37] USAGE, https://developer.wunderkind.co/docs/websdk-usage#login

51. As industry leaders,[38] trade groups,[39] and courts[40] agree, an ordinary person can use an email address to uniquely identify another individual. Indeed, there exists multiple services that enable anyone with internet access and a credit card to look up who owns a particular email address.[41]

52. Although Defendant collects "hashed" e-mail addresses, the FTC has warned companies for over a decade—including as recently as July 24, 2024—that hashing is an insufficient method of anonymizing information. As the FTC has noted, "hashes aren't "anonymous" and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized."[42]

53. Similarly, back in 2012, the FTC warned that "hashing is vastly overrated as an 'anonymization' technique" and that "the casual assumption that hashing is sufficient to anonymize data is risky at best, and usually wrong."[43]

54. Why is this so? "Once an email address is known, it can be hashed and compared against supposedly 'anonymous' hashed email addresses. This can be done by marketing or

---

[38] Allison Schiff, *Can Email Be The Next Big Online Identifier?*, AD EXCHANGER (Aug. 25, 2020), https://www.adexchanger.com/data-exchanges/can-email-be-the-next-big-online-identifier/ (quoting Tom Kershaw, CTO of Magnite, who said "[a]n email address is universally considered to be PII, so as such it can never be a valid identifier for online advertising").

[39] Network Advertising Initiative, NAI CODE OF CONDUCT 19 (2020), https://thenai.org/wp-content/uploads/2021/07/nai_code2020.pdf (identifying email as PII).

[40] *See United States v. Hastie*, 854 F.3d 1298, 1303 (11th Cir. 2017) ("Email addresses fall within the ordinary meaning of information that identifies an individual. They can prove or establish the identity of an individual.").

[41] *See*, *e.g.*, BEENVERIFIED, https://www.beenverified.com/.

[42] Staff in the Office of Technology, *No, Hashing Still Doesn't Make Your Data Anonymous*, FTC (July 24, 2024), https://tinyurl.com/53ecdrff.

[43] Ed Felten, *Does Hashing Make Data "Anonymous"?*, FTC (Apr. 22, 2012), https://tinyurl.com/mt9xsm4z.

advertising companies that use hashed email addresses as identifiers, or hackers who acquire hashed addresses by other means."[44]

55. Indeed, "[f]rom a computer science perspective, the claim that a hashed email address is not personally identifying is patently false."[45]

> What if you have data associated with a hash of an unknown email address and want to recover the original address? It's surprisingly easy: you can rent a multi-GPU virtual machine for $14.40 an hour, which gives you 73 billion MD5 hash computations per second based on published benchmarks. Modern methods have gotten really good at enumerating plausible sequences of characters and numbers in passwords, and we believe these methods will extend to email addresses. If they do, it would mean that email address hashes can be broken much more efficiently than through brute forcing (i.e., trying all possible combinations of characters). *We posit that with a trillion guesses — a cost of 6 US cents — it should be possible to enumerate the majority of email address in use*.[46]

56. Given the availability online of such "leaked" email/hashed email matches, entities are merely "pretend[ing]to protect your privacy"[47] through SHA-256 and/or other hashing algorithms.

---

[44] Gunes Acar, *Four Cents To Deanonymize: Companies Reverse Hashed Email Addresses*, CITP BLOG (Apr. 9, 2018), https://blog.citp.princeton.edu/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/.

[45] Steven Englehart, *I never signed up for this! Privacy implications of email tracking*, CITP BLOG (Sept. 28, 2017), https://blog.citp.princeton.edu/2017/09/28/i-never-signed-up-for-this-privacy-implications-of-email-tracking/.

[46] *Id.* (emphasis added).

[47] *Id.*

57. This is especially true for Defendant when one of its data sub-processors, a third-party data processor engaged by a data processor who has or will have access to or process personal data from a data controller,[48] is Google Cloud.[49]

58. Google informs advertisers who wish to "target[] Customer Match segments in [] Google Ads campaigns[]" that "Google keeps track of the email addresses and phone numbers for Google accounts and the corresponding hashed strings for those email addresses or phone numbers."[50] Accordingly, Google can compare "each hashed string on [a given email] list with the hashed string for email address or phone number of Google accounts[]" to determine "[i]f there's a match[with a] … corresponding Google account[.]"[51]

59. Thus, even in hashed form, e-mail addresses are traceable to individuals.

B. Cookies

60. Another persistent identifier that Defendant collects is a browser "cookie." "Cookies are bits of data that are sent to and from your browser to identify you. When you open a website, your browser sends a piece of data to the web server hosting that website."[52]

61. Defendant uses several cookies, including but not limited to the 'BxID' cookie, which is the "statistical identifier."[53] Defendant says this cookie is "created when our systems

---

[48] *Subprocessor*, GDPR, https://www.gdprsummary.com/gdpr-definitions/sub-processor/ (last visited June 2, 2025).

[49] *Data Subprocessors*, WUNDERKIND, https://www.wunderkind.co/privacy/data-subprocessors/ (last visited June 2, 2025).

[50] *About the customer Matching Process*, GOOGLE, https://support.google.com/google-ads/answer/7474263 (last visited June 2, 2025).

[51] *Id.*

[52] *What are cookies?*, MICROSOFT, https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies?form=MA13I2 (last visited Dec. 23, 2024).

[53] *Wunderkind Privacy Policy*, WUNDERKIND, https://www.wunderkind.co/privacy/ (last visited Feb. 11, 2025).

read pseudonymous information about your computer or device, including the user agent, IP address, and the browser and operating system of your computer and device."[54]

62. Using this information, Defendant "determine[s] within a reasonable level of certainty that [it is] encountering the same computer or device, including in environments where third-party cookies are not supported"[55]

63. When a user visits a website participating in the Wunderkind ad exchange, the owner of the website partnering with Wunderkind requests that Defendant sets a cookie onto the browser or device of the person visiting the website. After the cookie is loaded onto a person's browser, each time that person visits a website where Defendant is operating, Defendant uses the cookie to identify the website visitor as the same person who visited previous websites with the same cookie installed on their browser. As such, Wunderkind is able to track each individual internet user across multiple sites to create a more detailed profile on that person's beliefs, interests, and habits.

64. This information is cross-referenced with other information collected by Defendant to specifically identify the individual using the device and to add this web-activity information to a larger profile on the individual in order to sell their profile for targeted advertising.

C. IP Addresses

65. IP addresses are another common persistent identifier.

66. An IP address is a unique set of numbers assigned to a device on a network, which is typically expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The traditional format of IP addresses is called IPv4, and it has a finite amount of combinations and

[54] *Id.*

[55] *Id.*

thus is limited to approximately 4.3 billion addresses. Because this proved to be insufficient as the Internet grew, IPv6 was introduced. IPv6 offers a vastly larger address space with 340 undecillion possible addresses. While IPv6 adoption has been increasing, many networks still rely on IPv4.[56]

67. Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices.

68. IP addresses are not freely accessible. If an individual is not actively sending data packets out, their IP address remains private and is not broadcast to the wider internet.

69. IP addresses can be used to determine the approximate physical location of a device. For example, services like iplocation.io[57] use databases that map IP addresses to geographic areas—often providing information about the country, city, approximate latitude and longitude coordinates, or even the internet service provider associated with the public IP.

70. Thus, knowing a user's public IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."[58]

71. An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[59] and (ii) "to target specific households, businesses[,] and

---

[56] *See, e.g.*, https://www.cloudflare.com/learning/network-layer/internet-protocol/ (last visited Dec. 23, 2024); https://netbeez.net/blog/rfc1918/ (last visited Dec. 23, 2024).

[57] https://iplocation.io/ (last visited Dec. 23, 2024).

[58] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://tinyurl.com/4ubds52w (as accessed Dec. 9, 2023).

[59] *Location-Based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/ (last visited June 3, 2025).

even individuals with ads that are relevant to their interests."[60] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[61] because "[c]ompanies can use an IP address … to personally identify individuals."[62]

72. In fact, an IP address is a common identifier used for "geomarketing," which is "the practice of using location data to identify and serve marketing messages to a highly-targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by targeting them based on location-related factors, enabling [websites] to tailor your marketing to the products or services that appeal to their needs.."[63] For example, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[64]

73. "IP targeting is a highly effective digital advertising technique that allows you to deliver ads to specific physical addresses based on their internet protocol (IP) address. IP targeting technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads to specific households or businesses based on their location."[65]

---

[60] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://tinyurl.com/4hjxwse8.

[61] *IP Targeting: Understanding This Essential Marketing Tool*, *supra*, https://tinyurl.com/4ubds52w.

[62] Trey Titone, *The Future Of IP Address As An Advertising Identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

[63] *See*, *e.g.*, *The Essential Guide to Geomarketing: Strategies, Tips & More*, DEEP SYNC (Nov. 20, 2023), https://deepsync.com/geomarketing/.

[64] *See*, *e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.

[65] *IP Targeting*, SAVANT DSP, https://tinyurl.com/67ahreuw.

74. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographics or behavioral data."[66]

75. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's IP address because it "can be more cost-effective than other forms of advertising."[67] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[68]

76. In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[69] "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[70]

77. Putting IP addresses in the hands of a data broker like Defendant is particularly invasive, as the NATO report noted:

> [a] data broker may receive information about a[] [website] user, including his … IP address. The user then opens the [website] while his phone is connected to his home Wi-Fi network. When this happens, the data broker can use the IP address of the home network to identify the user's home, and append this to the unique profile it is compiling about the user. If the user has a computer connected to the same network, this computer will have the same IP address. The data broker can then use the IP address to connect the computer to the same user, and identify that user when their IP address makes requests on other publisher pages within their ad network. Now the data broker knows that the same individual is using both the phone and the computer, which allows it to track behavior across devices

[66] *Id.*

[67] Williams, *supra*, https://tinyurl.com/4hjxwse8.

[68] *Id.*

[69] *Id.*

[70] *Id.*

> and target the user and their devices with ads on different networks.[71]

78. For these reasons, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual."[72]

79. Likewise, under the California Consumer Privacy Act, IP addresses are considered "personal information" because they are "reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1)(A).[73]

D. Universal Resource Locator

80. In addition to collecting a myriad of identifiers, Wunderkind's Advertising Partners' tags and tag manager solutions collect the Universal Resource Locator (URL) of the webpages visited by each individual.

81. Sometimes known as a "web address," the URL is the name of the webpage as displayed in the address bar of a browser.

82. Each page on a website has its own individual URL, allowing tags with access to the URL to see which pages of a website a particular internet user visited.

83. All URLs identify the pages of each page of a website an internet user visited.

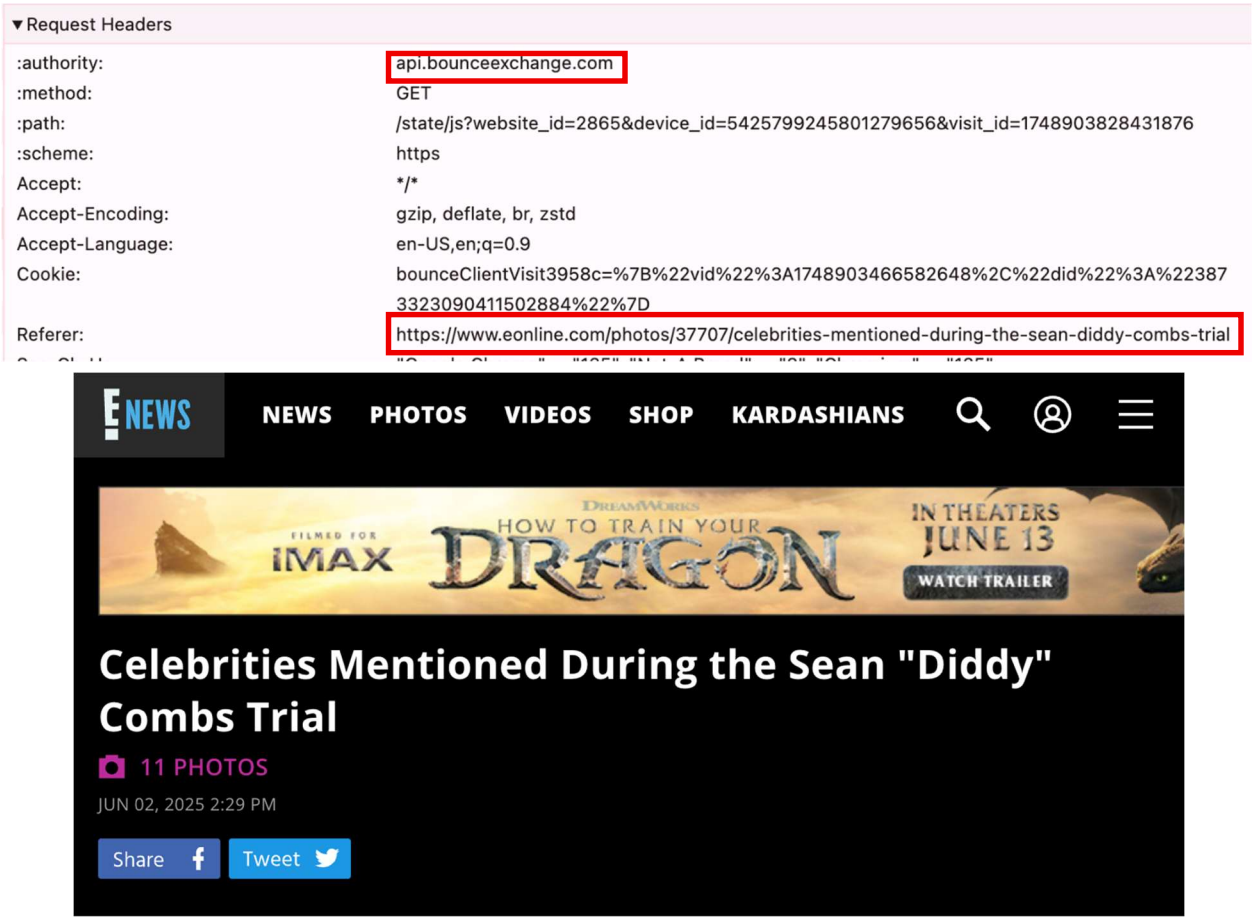
---

[71] TWETMAN & BERGMANIS-KORATS, *supra*, at 11.

[72] IS AN IP ADDRESS PERSONAL DATA?, CONVESIO, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/ (last visited June 3, 2025); *see also* WHAT IS PERSONAL DATA?, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en (last visited June 3, 2025).

[73] A "consumer" is defined as "a natural person who is a California resident." Cal. Civ. Code § 1798.140(i).) A "household" is defined as "a group … of consumers who cohabitate with one another at the same residential address and share use of common devices or services." Cal. Civ. Code § 1798.140(1).)

84. For example, when viewing an article on the E! Online website, the full name of the Article is included in the URL captured by Defendant.



85. As such, any tag that intercepts the URL on this page also intercepts the titles of the content the users view. This process works similarly on other websites.

86. Wunderkind, through its Advertising Partners' tags and tag manager solutions, collects the URLs and any information that can be gleaned or inferred from those URLs are added to the profiles that Defendant has for that particular user.

E. Mobile Advertising Identifiers

87. Defendant employs similar methods to track individuals using mobile apps on Android and iOS devices.

88. Defendant owns and operates "software development kits" (SDKs), pieces of code that work independently or with "application programming interfaces" (APIs) and are loaded into mobile apps and can track users' activity on certain apps.[74]

89. An SDK is a "set of tools for developers that offers building blocks for the creation of an application instead of developers starting from scratch … For example, Google Analytics provides an SDK that gives insight into user behavior, engagement, and cross-network attribution."[75]

90. An API "acts [as] an intermediary layer that processes data transfer between systems, letting companies open their application data and functionality to external third-party developers [and] business partners."[76] An API can "work[] as a standalone solution or included within an SDK … [A]n SDK often contains at least one API."[77] APIs "enable[] companies to open up their applications' [or websites'] data and functionality to external third-party developers, business partners, and internal departments within their companies."[78]

---

[74] *SDK vs. API*, IBM, https://www.ibm.com/blog/sdk-vs-api/ ("SDK" stands for software development kit and "is a set of software-building tools for a specific program," while "API" stands for application programming interface) (last accessed Dec. 23, 2024). Plaintiffs will refer to both collectively as the "Bounce Exchange Tracker" to avoid any confusion.

[75] *API vs. SDK: The Difference Explained (With Examples)*, GETSTREAM, https://getstream.io/glossary/api-vs-sdk/ (last accessed June 2, 2025).

[76] *What is an API?*, IBM, available https://www.ibm.com/topics/api (last accessed June 2, 2025).

[77] *SDK VS. API: WHAT'S THE DIFFERENCE?*, IBM (July 13, 2011), https://www.ibm.com/blog/sdk-vs-api/ ("SDK" stands for software development kit and "is a set of software-building tools for a specific program," while "API" stands for application programming interface).

[78] *Application Programming Interface (API)*, IBM, https://www.ibm.com/cloud/learn/api (last accessed June 2, 2025).

91. Defendant explains that "[a]n SDK for iOS and Android that captures user behavior, enabling push notifications, in app messaging, and identity resolution for personalized marketing[.]"[79]

92. For example, Defendant collects advertising identifiers that are designed to track the app activity of individual users across different apps. Two of the most prominent are AAIDs (for Android devices) and IDFAs (for iOS devices) (collectively, "Mobile Advertising IDs" or "MAIDs").[80]

93. An AAID is a unique string of numbers which attaches to a device. As the name implies, an AAID is sent to advertisers and other third parties so they can track user activity across multiple mobile applications.[81] So, for example, if a third party collects AAIDs from two separate mobile applications, it can track, cross-correlate, and aggregate a user's activity on both apps.

94. Although technically resettable, an AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets that identifier. The fact that the use and disclosure of AAIDs is so ubiquitous evinces an understanding on the part of Defendant, Google, and others in the field that they are almost never manually reset by users (or else an AAID would be of no use to advertisers). Byron Tau, MEANS OF CONTROL: HOW THE HIDDEN ALLIANCE OF TECH AND GOVERNMENT IS CREATING A NEW AMERICAN SURVEILLANCE STATE at 175 (2024) ("Like me, most people had no idea about the 'Limit Ad Tracking' menu on

[79] *Build*, WUNDERKIND, https://www.wunderkind.co/platform/build/ (last accessed June 2, 2025).

[80] [80] SDK VS. API: WHAT'S THE DIFFERENCE?, IBM (July 13, 2011), https://www.ibm.com/blog/sdk-vs-api/ ("SDK" stands for software development kit and "is a set of software-building tools for a specific program," while "API" stands for application programming interface).

[81] *Support*, GOOGLE, https://support.google.com/googleplay/android-developer/answer/6048248 (last visited Dec. 23, 2024).

their iPhones or the AAID that Google had given even Android devices. Many still don't."); *see also Louth v. NFL Enterprises LLC*, 2022 WL 4130866, at *3 (D.R.I. Sept. 12, 2022) ("While AAID are resettable by users, the plaintiff plausibly alleges that AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets their AAID.") (cleaned up).

95. Using publicly available resources, an AAID can track a user's movements, habits, and activity on mobile applications.[82] Put together, the AAID serves as "the passport for aggregating all of the data about a user in one place."[83]

96. Because an AAID creates a record of user activity, this data can create inferences about an individual, like a person's political or religious affiliations, sexuality, or general reading and viewing preferences. These inferences, combined with publicly available tools, make AAIDs an identifier that sufficiently permits an ordinary person to identify a specific individual.

97. Similarly, an "Identifier for Advertisers, or IDFA for short, is a unique, random identifier (device ID) that Apple assigns to every iOS device. An IDFA would be the equivalent of a web cookie, in the sense that it enables advertisers to monitor users' engagement with their ads, and keep track of their post-install activity."[84]

98. Defendant's collection of IDFAs allows Wunderkind to track iOS users' activity across the various apps they use. Like the AAID, this data can create inferences about an

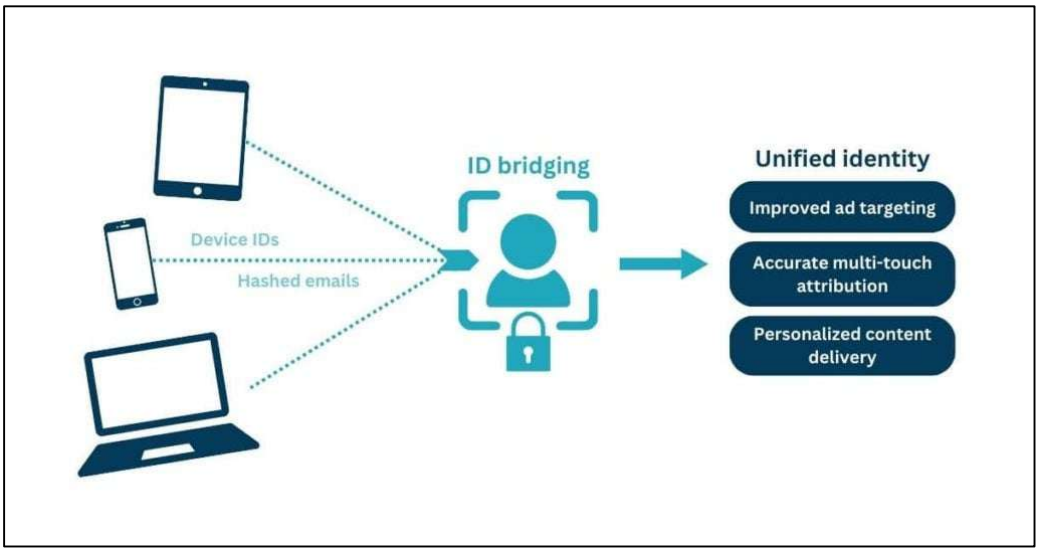
[82] *Using just 1000 worth of mobile adverts you can effectively track anyone*, HUFFINGTON POST, https://www.huffingtonpost.co.uk/entry/using-just-1000-worth-of-mobile-adverts-you-can-effectively-track-anyone_uk_59e87ccbe4b0d0e4fe6d6be5 (last visited Dec. 23, 2024).

[83] *Trend Report: Apps Oversharing Your Advertising ID*, DIGITAL WATCHDOG, https://digitalwatchdog.org/trend-report-apps-oversharing-your-advertising-id/ (last visited Dec. 23, 2024).

[84] IDFA, APPSFLYER GLOSSARY, https://www.appsflyer.com/glossary/idfa (last visited Dec. 23, 2024).

individual, such as a person's political or religious affiliations, sexuality, or general reading and viewing preferences. These inferences, combined with publicly available tools, sufficiently permits even an ordinary person to identify a specific individual with the IDFA.

99. Regardless of whether these IDs are supposed to be anonymous, MAIDs are often combined with other identifiers to identify users in what is known as ID Bridging.



100. "ID Bridging" is the process of "piecing together different bits of information about" a user "to confidently infer that it is the same individual accessing a publisher's site or sites from various devices or browsers."[85] That is, users can be identified and tracked by "bridging" (or linking) their MAIDs to other sources, such as e-mail addresses, geolocation, or phone numbers.

101. ID Bridging "has long been the foundation of programmatic advertising,"[86] which is the process by which companies "use [] advertising technology to buy and sell digital ads" by "serv[ing] up relevant ad impressions to audiences through automated steps, in less than a

[85] Kayleigh Barber, *WTF Is The Difference Between Id Bridging And Id Spoofing?*, DIGIDAY (July 8, 2024, https://digiday.com/media/wtf-is-the-difference-between-id-bridging-and-id-spoofing/.

[86] https://www.adexchanger.com/data-driven-thinking/how-can-id-bridging-the-foundation-of-our-space-suddenly-be-a-bad-thing/.

second."[87] It entails a "unique identifier[] assigned to individual devices," including "Google's Advertising ID," personal information like geolocation and e-mail address, and "cross-platform linkage."[88]

102. ID Bridging is a money-making machine for advertisers and app developers. On the advertiser side, ID Bridging "increase the chances of an ad buying platform finding their inventory to be addressable and, therefore, maximizes their 'ad yields.'" And on the app developer side, "publishers can boost revenue from direct-sold campaigns by offering advertisers access to more defined and valuable audiences."[89]

103. In other words, advertisers will be able to find users that are more directly and likely interested in what is being sold by having access to significantly more information. And app users' information will be more valuable (and therefore, bring in more money to app developers) because it is combined with a plethora of other information from various sources.

104. Put simply, ID bridging enables the supply-side to extend user identification beyond the scope of one browser or device.[90]

105. Yet, while those within the ID Bridging industry describe it as privacy-protective, it is anything but. As courts have noted, the "ability to amass vast amounts of personal data for

---

[87] PROGRAMMATIC ADVERTISING, https://tinyurl.com/37hwcrx9.

[88] Anete Jodzevica, I*D Bridging: The Privacy-First Future of Audience Targeting*, SETUPAD (Nov. 15, 2024), https://setupad.com/blog/id-bridging/. Ironically, the example given in this article is a "hashed e-mail," where the e-mail Defendant collected in this example is not hashed.

[89] Bennett Crumbling, *What Is 'ID Bridging' And How Publishers Use It To Grow Direct And Programmatic Revenue?*, OPTABLE (Aug. 22, 2024. https://www.optable.co/blog/what-is-id-bridging.

[90] *See, e.g.*, Budi Tanzi, *New OpenRTB Specs Ensure Identity Resolution Can Be Done Transparently With Trusted Partners*, EXPERIAN (Dec. 18, 2024), https://www.experian.com/blogs/marketing-forward/new-openrtb-specs-ensure-identity-resolution-can-be-done-transparently-with-trusted-partners/.

the purpose of identifying individuals and aggregating their many identifiers" creates "dossiers which can be used to further invade [users] privacy by allowing third parties to learn intimate details of [users'] lives, and target them for advertising, political, and other purposes, ultimately harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them." *Katz-Lacabe v. Oracle Am., Inc.*, 688 F. Supp. 3d 928, 940 (N.D. Cal. 2023) (cleaned up).

106. In February 2019, Oracle published a paper entitled "Google's Shadow Profile: A Dossier of Consumers Online and Real World Life," part of which provides as accurate a description of Google's services:

> a consumer's "shadow profile" [is a] massive, largely hidden dataset[] of online and offline activities. This information is collected through an extensive web of … services, which is difficult, if not impossible to avoid. It is largely collected invisibly and without consumer consent. Processed by algorithms and artificial intelligence, this data reveals an intimate picture of a specific consumer's movements, socio-economics, demographics, "likes", activities and more. It may or may not be associated with a specific users' name, but the specificity of this information defines the individual in such detail that a name is unnecessary.[91]

107. In other words, ID Bridging is dangerous because of the sheer expanse of information being compiled by companies like Defendant without the knowledge or consent of users, all of which is being done for Defendant's pecuniary gain.

III. DEFENDANT MATCHES PLAINTIFF'S AND CLASS MEMBERS' PERSONAL INFORMATION TO COMPREHENSIVE USER PROFILES

108. Once Defendant collects information from website users, it uses these various identifiers to compile and tie consumers to comprehensive user profiles that are offered up for sale.

[91] GOOGLE'S SHADOW PROFILE: A DOSSIER OF CONSUMERS ONLINE AND REAL WORLD LIFE at 1 (Feb. 2019), https://tinyurl.com/2mtuh7vf.

109. Defendant is a data broker and "behavioral automation software and analytics company … [that] help[s] website publishers … drive higher engagement from their website visitors … via [Defendant's] behavioral automation platform, identity platform, ad serving platform, and performance advertising platform."[92]

110. To do so, Defendant's technology "recognizes [clients'] website traffic" (*i.e.*, who each individual user is), so that clients can serve targeted ads.[93] Defendant "host[s] the largest first-party data set out of comparable solution[s] on the market."[94] This enables Defendant's "1,000+ clients with more powerful tools to recognize consumers, collect first-party data, and deliver better, more personalized experiences at scale."[95]

111. Wunderkind collects personal information including but not limited to "[b]rowsing history, search history, [and] information on a consumer's interaction with a website, application, or advertisement" and "may transfer data collected through … [Wunderkind's] marketing activities to entities such as "(i) website analytics vendors, who collect cookie and website engagement information to help understand website performance, (ii) advertising vendors, who collect cookie and website engagement information to target relevant advertising, and (iii) email marketing and lead database vendors, who collect email address and other personal information to improve email marketing efforts."[96]

---

[92] *Privacy Policy*, WUNDERKIND, https://www.wunderkind.co/privacy/ (last accessed May 27, 2025).

[93] *Wunderkind Drives Unmatched Revenue*, WUNDERKIND, https://www.wunderkind.co/performance-marketing-solutions-for-ecommerce/ (last visited Jan. 22, 2025).

[94] *Id.*

[95] *Wunderkind Unveils Identity Solution Enhancements To Amplify Customer Revenue and Experiences*, BusinessWire (Sept. 25, 2024), https://tinyurl.com/38kk9jfb.

[96] *Id*.

112. Defendant then matches the information it collects from users of its' clients websites (*e.g.*, the IP addresses and device metadata of website users) with its data set of "9 billion consumer devices and 1 billion consumer profiles," which Wunderkind "stores [] in [its] database."[97]

113. As Defendant notes, this repository of information is "more than most identity solutions have collected in their existence."[98] Indeed, as Wunderkind describes it:

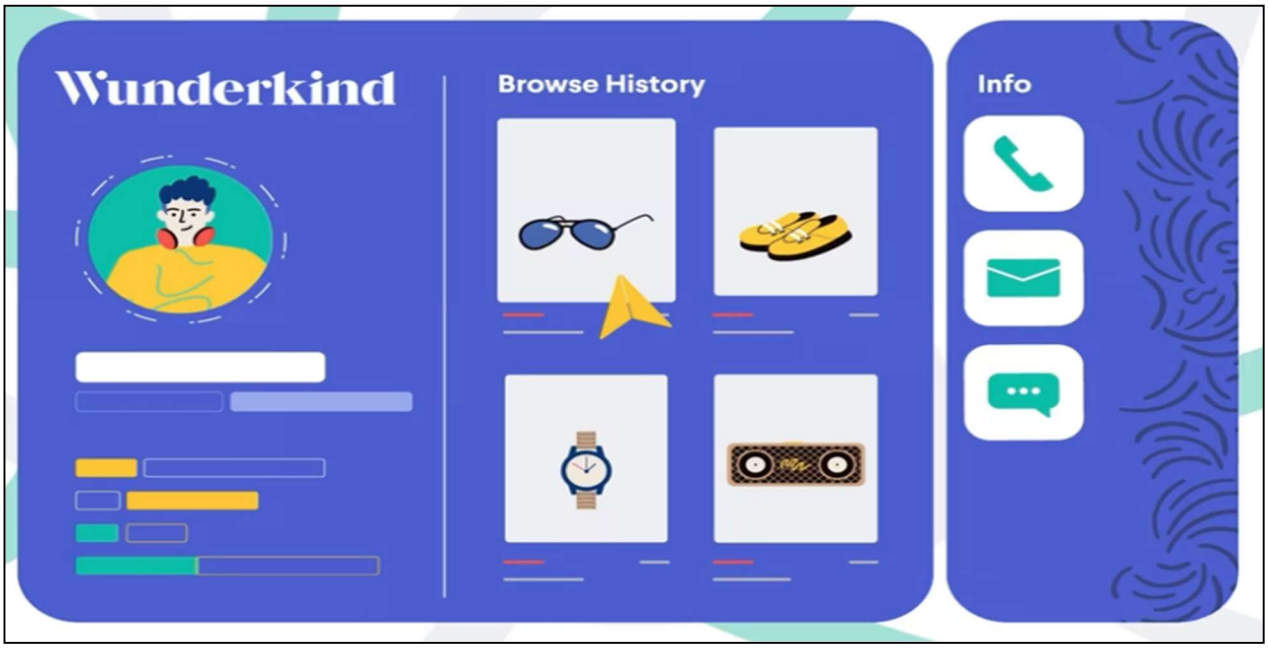
> Identity resolution is the missing puzzle piece that bridges the gap between anonymous browsing and targeted engagement.
>
> At Wunderkind, we define identity resolution as the process of tying an online visitor to an email address and phone number.[99]

[97] *Id.* (emphasis added).

[98] *The Value of Cookies Plummets, But Identity Resolution Saves the Day*, WUNDERKIND (Aug. 23, 2024), https://tinyurl.com/4zw42xd7.

[99] *Why Identity Resolution is the New Tool in Travel Marketing*, WUNDERKIND, https://www.wunderkind.co/blog/article/why-identity-resolution-is-the-new-tool-in-travel-marketing/ (last accessed June 2, 2025).

114. Defendant then "analyze[s] everything about visitor behavior, from purchase history to traffic sources to engagement patterns to even the moment a visitor is abandoning a site using its patented exit-intent technology," and "then uses that information to inform a variety of customer acquisition strategies designed to dramatically boost key business metrics for [Defendant's] clients."[100]



115. More specifically, Defendant offers the "Wunderkind Identity" suite of services, which includes the following services that Wunderkind provides to its clients:

116. **The Unified Identity Graph** is Wunderkind's PrivacyID that consolidates emails, phone numbers, DeviceIDs, browsing history, shopping preferences, and third-party identifiers

[100] *Bounce Exchange (Past Sponsor)*, ETAIL CONNECT, https://etailconnectwest.wbresearch.com/sponsors/bounce-exchange (last accessed June 2, 2025); *see also* HOW WUNDERKIND DRIVES GUARANTEED REVENUE, https://youtu.be/_pbBYDYs8mE?si=RqBULPGM26M5GIlV&t=56.

into a single graph powered by proprietary machine learning algorithms, significantly increasing identity rates.[101]

117. **Server-Side Tracking** extends visitor recognition across multiple visits, improving onsite experiences through essential first-party cookies and ensuring a seamless customer journey across channels.[102]

118. **Cross-Site and Device Identification** allows Wunderkind to leverage probabilistic and deterministic methods to identify traffic across sites and devices down to an email address or phone number in customer databases.[103]

119. **Identity Enrichment Ecosystem** enables advertisers to use identity frameworks like LiveRamp and UID2 for scalable, cookie-less targeting in programmatic ads, while publishers can convert unknown visitors into addressable audiences, boosting CPMs.[104]

120. The last of the above services bears additional emphasis. LiveRamp is another registered data broker, while the UID2 is an identifier operated by The Trade Desk, another ad-tech company focused on data monetization and consumer de-anonymization.[105] So, Defendant (already a massive data broker) syncs its information with the information known about users by LiveRamp and The Trade Desk, which is extensive.

---

[101] *Wunderkind Unveils Identity Solution Enhancements To Amplify Customer Revenue and Experiences*, BusinessWire (Sept. 25, 2024), https://tinyurl.com/38kk9jfb.

[102] *Id*.

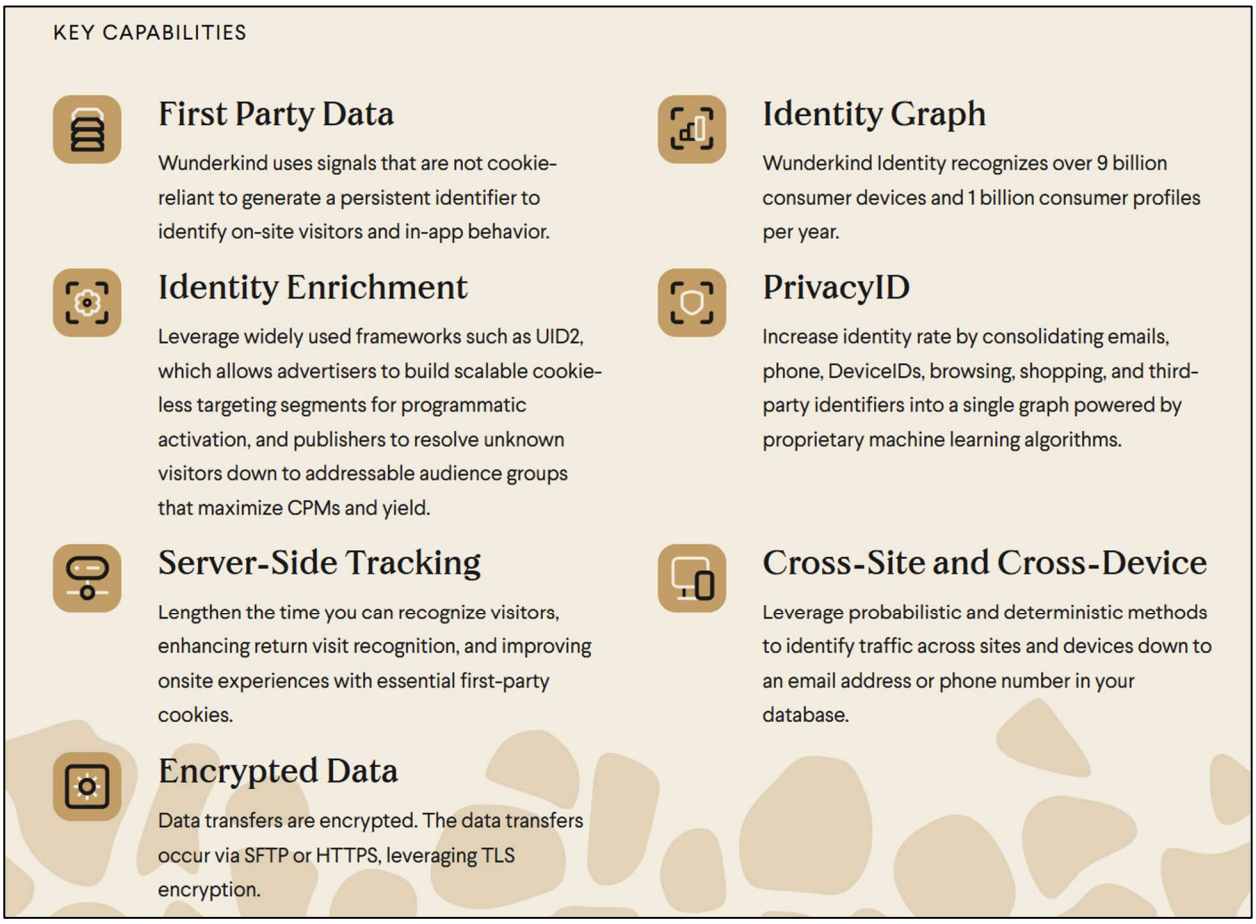
[103] *Id*.

[104] *Id*.

[105] *See* DATA BROKER REGISTRATION FOR LIVERAMP, INC., https://oag.ca.gov/data-broker/registration/560496 (last visited June 3, 2025); *The Trade Desk's Privacy Crisis: Lawsuits Expose Adtech's Data Dilemma*, CAPTAIN COMPLIANCE (Apr. 17, 2025), https://captaincompliance.com/education/the-trade-desks-privacy-crisis-lawsuits-expose-adtechs-data-dilemma/.

121. In fact, Defendant specifically touts its integrations with LiveRamp and The Trade Desk, even noting that "LiveRamp's identification quality may not match the granularity of Wunderkind's proprietary first-party Identity Graph" that Wunderkind provides to clients like Defendant.[106]

122. Defendant also provides what it ironically calls a "PrivacyID," which "[i]ncrease[s] identity rate by consolidating emails, phone, DeviceIDs, browsing, shopping, and third-party identifiers [*i.e.*, the various permanent identifiers described above] into a single graph powered by proprietary machine learning algorithms."[107]



[106] Sarah Hall, *Wunderkind's Identity Enrichment: Boosting Identification and Revenue Through Strategic Partnerships*, WUNDERKIND (Sep. 23, 2024), https://tinyurl.com/y48kdbds.

[107] WUNDERKIND IDENTITY, https://www.wunderkind.co/platform/identity/

123. Defendant goes on to admit exactly what Plaintiff has alleged herein: that it enriches user data to "be passed into the programmatic ad ecosystem [*i.e.*, real-time bidding], enabling our publisher clients to command higher CPMs from advertisers, resulting in a direct increase in revenue."[108] As Defendant admits, its "identity enrichment" efforts "provide[] publishers with richer user data, empowering them to attract more advertisers and increase the value of their ad inventory."[109]

124. Further, Defendant admits its identity resolution services:

> help identify a large percentage of a brand's website traffic by *matching the devices visiting the site back to a consumer's email address or phone number*, without relying solely on third-party cookies. Because Identity Resolution partners track consumer behavior across thousands of websites and ad networks they understand the multiple devices a consumer uses and stores a consumer's browse, click and purchase behavior at an individual level within their identity graph.[110]

125. In sum, when users visit a website with Defendant's trackers loaded onto it, Defendant collects various bits of information from users that are matched with and compiled into comprehensive user profiles. Those profiles de-anonymize and identify users and paint a thorough picture of the user's various interests, habits, affiliations, and identities. And Defendant provides those profiles to the Partner Pixels for the serving of advertisements, and advertisers can better target users based on this enriched data, (for which they will pay more money as a result). Thus drives the profits of Defendant's website clients and makes Defendant's services more useful, allowing Defendant to broaden its identity network. All of this comes at the expense of internet users, whose privacy is invaded and whose consent is not procured.

---

[108] Hall, *supra*, https://tinyurl.com/y48kdbds.

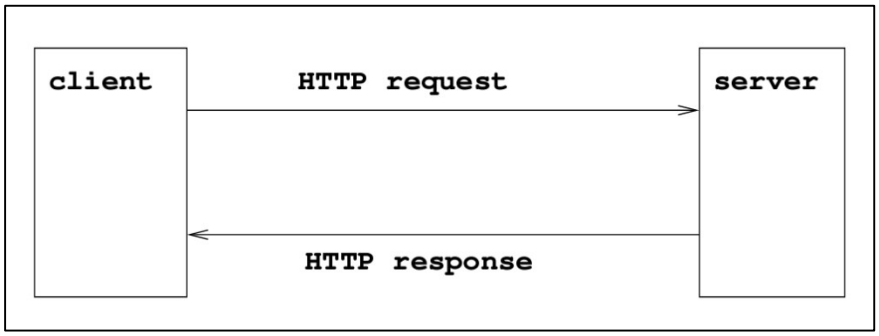
[109] *Id*.

[110] *The Value of Cookies Plummets, But Identity Resolution Saves the Day*, *supra* (emphasis added).

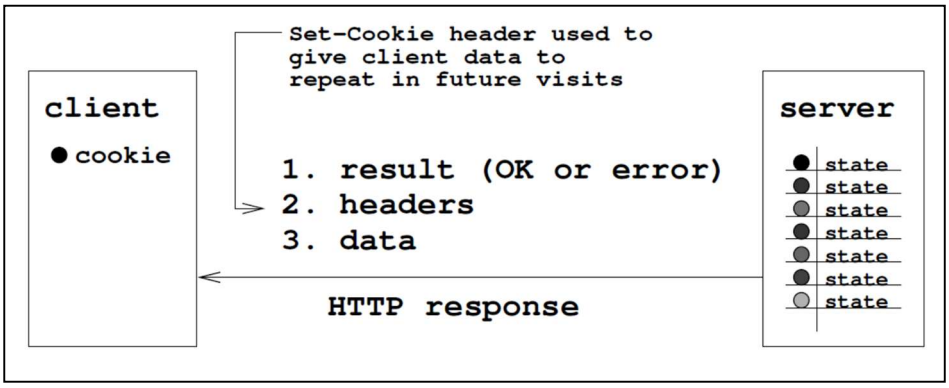
126. All of the above information is used to identify individuals and track their activity, but persistent identifiers and URL information play particular roles in the Wunderkind surveillance apparatus.

IV. DEFENDANT SYNCS ITS COMPREHENSIVE USER PROFILES WITH THE PARTNER PIXELS TO SELL USER INFORAMTION TO ADVERTISERS ON THE PARNTER WEBSITES

127. To make a website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to the website's server where the relevant website data is stored. In response to the request, the website's server sends an "HTTP response" back to the browser with a set of instructions.



128. The server's instructions include how to properly display the website—*e.g.*, what images to load, what text should appear, or what music should play. In addition, the website server's instructions cause the Defendant's tracker (if integrated on the website) to be installed on a user's browser.



129. Defendant's tracker then causes the browser to send the identifying information described above to Defendant to de-anonymize and identify the user, which is then used to compile a profile that is sold to advertisers.

130. Further, through cookie syncing, Defendant shares these comprehensive user profiles and replete database of personal information with the Partner Pixels. And the Partner Pixels use this information to solicit higher bids from advertisers by enabling advertisers to identity, and thus, better target website users.

131. As part of their investigation, Plaintiff's counsel conducted testing on several websites to provide a sample of the widespread tracking and wiretapping of, and targeted advertising to, millions of Americans by Defendant. Those websites include but are not limited to: E! Online.

132. However, there are hundreds or thousands of others where the same or similar information is collected and the same process occurred. All of these websites collectively are referred to as the "Partner Websites."

A. E! Online

133. As an example, Defendant's tracker is operating on E! Online, which is a website, accessible at https://www.eonline.com/, that reports on entertainment, pop culture, and lifestyle trends.[111]

134. Unbeknownst to website visitors, Defendant's tracker is loaded onto each page of the E! Online website:

GET	tag.bounceexchange.com
GET	assets.bounceexchange.com

[111] *About,* E! ENTERTAINMENT TELEVISION, LLC, https://www.eonline.com/about (last visited Jan. 22, 2024).

135. Upon being loaded on the E! Online website, Defendant collects through its collects a variety of information about the user, including but not limited to the user's IP address and device information (browser, version, platform, and device type). The below screenshot of traffic from Plaintiff's browser on the E! Online website is illustrative[112]:


```
"device": {
  "browser": "Safari",
  "version": "605.1.15",
  "platform": "Mac OS X",
  "device_type": "desktop"
},
"no_kinesis": true,
"request_token": "18351d509014cd3ee657cf5a951f3d7714df8a54743259ddc62496b1893be9c8",
"mobile": false,
"vip": "146.[redacted],
```


136. As described above, Defendant used this information to link Plaintiff to a profile it maintained on her that allowed her to be de-anonymized and identified. Defendant then provided this profile to several Partner Pixels through cookie syncing: PubMatic, Magnite, and Criteo.


```
"pbm": {
    "desktop_id": "",
    "mobile_id": "",
    "publisher_id": "156512",
    "qa_site_id": "248764",
    "reload": 300000,
    "timeout": 2000,
    "endpoint": "hbopenbid.pubmatic.com\/translator?",
    "user_sync_endpoint": "ads.pubmatic.com\/AdServer\/js\/user_sync.html",
    "ssp_priority": 1
},
"criteo": {
    "network_id": "11254",
    "publisher_id": "WKNDdefault",
    "ssp_priority": 5
},
"magnite": {
    "account_id": "20986",
    "reload": "300000",
    "site_id": "",
    "zone_id": "",
    "ssp_priority": 7
```


[112] All but the first three digits of the user's IP address have been redacted throughout this Complaint to protect their privacy.

137. These are only the Partner Pixels identified during a single session on website. There are likely dozens more partner pixels that exchange Plaintiff's and Class Members' information with Defendant on hundreds of websites.

1. Pubmatic

138. For example, as the above screenshot indicates, Defendant syncs its tracker with another tracker installed on the E! Online website that is operated by PubMatic, who is also a registered data broker in California.[113]

139. PubMatic describes itself as a digital advertising platform that "exist[s] to enable content creators to run a more profitable advertising business, which in turn allows them to invest back into the multi-screen and multi-format content that consumers demand."[114]

140. Specifically, PubMatic is a "supply side platform" that helps website operators like Defendant "[m]aximize advertising revenue and control how your audiences are accessed."[115] To do this, PubMatic provides a "unique, supply path optimized and addressable brand demand—from the SSP of choice for the top advertisers and agencies in the world."[116]

141. Likewise, PubMatic provides identity resolution services via its "Identity Hub", "a leading ID management tool for publishers that leverages specialized technology infrastructure to simplify the complex alternative identifier marketplace."[117] This allows website operators like

---

[113] DATA BROKER REGISTRATION FOR PUBMATIC, INC., https://oag.ca.gov/data-broker/registration/186702.

[114] *The Supply Chain Of The Future*, PUBMATIC, https://pubmatic.com/about-us (last accessed Feb. 18, 2025).

[115] *The Digital Advertising Supply Chain of the Future. Delivered.*, PUBMATIC SSP, https://pubmatic.com/products/pubmatic-ssp-for-publishers/ (last accessed Feb. 18, 2025).

[116] *Id*.

[117] *Identity Management. Delivered.*, PUBMATIC, https://pubmatic.com/products/identity-hub/ (last accessed Feb. 18, 2025).

Defendant to "drive monetization in cookie-restricted environments" by "[c]onnect[ing] seamlessly with buyers to drive programmatic revenue."[118]

142. Notably, PubMatic also touts its ability to integrate with multiple other third parties—including "over 75 identity and data providers"—"leverage leading identifiers" to "help data owners [like Defendant] driver monetization and help media buyers [*i.e.*, advertisers] drive performance."[119]

143. PubMatic also helps advertisers select where to place their ads, to help companies "[s]mash [their] campaign KPIs [key performance indicators]" and "reach [their] target audiences more effectively."[120] One of the ways in which PubMatic accomplishes this is by selling "action packages," which are data sets—pulled together from different sources—to help advertisers target specific customers.[121] In other words, PubMatic utilizes third-party data, as well as data from the publisher where the ad is ultimately placed (*i.e.*, first-party), to determine where to place advertisers' ads and who to place them in front of.

144. By way of example, PubMatic sells a "Ramadan Auction Package" that targets consumers who observe Ramadan.[122] This package helps companies target people who have indicated interest in Ramadan Events through consumer behavior, have internet search history such as "Prayer & Fasting," have location data that is "[f]requently seen at places of worship," or

---

[118] *Id*.

[119] *Id*.

[120] *Connect With PubMatic's Auction Packages*, PubMatic, https://pubmatic.com/auction-packages (last visited Feb. 18, 2025).

[121] *Connect With PubMatic's Auction Packages*, PubMatic, https://pubmatic.com/auction-packages-apac (last visited Feb. 18, 2025).

[122] *Connect With PubMatic's Auction Packages: Ramadan*, PubMatic, https://pubmatic.com/auction-packages-apac (last visited Feb. 18, 2025).

have "[d]emographic data" that shows they are married or live with people "who have shown interest towards Ramadan."[123]

145. PubMatic touts its partnership with Wunderkind in a blog post, noting that the partnership "deliver[ed] greater scale via sell-side data targeting."[124]

146. The upshot of all this is that PubMatic enables website owners like E! Online to effectively sell their user inventory to advertisers in a de-anonymized, targeted format. By syncing its tracker with Defendant's tracker, PubMatic facilities this goal, leveraging Defendant's replete database of user profiles (described in more detail below) to de-anonymize and identify website users like users of the E! Online website.

147. Thus, when PubMatic offers Website users up for sale to advertisers—as is PubMatic's function as a supply-side platform—those users will receive higher bids because they can be better targeted by advertisers as a result of PubMatic's synchronization with Defendant. Defendant, in turn, builds on its already expansive database by learning whatever PubMatic knows about the user.

2. Criteo

148. As another example, as the above screenshot indicates, Defendant syncs its tracker with another tracker installed on the E! Online website that is operated by Criteo. Although Criteo is not a registered data broker, it is still involved in the selling and sharing of user information to advertisers.

---

[123] *Id.*

[124] *PubMatic and Wunderkind Deliver Greater Scale Via Sell-Side Data Targeting*, PUBMATIC, https://pubmatic.com/case-studies/pubmatic-and-wunderkind-deliver-greater-scale-via-sell-side-data-targeting/ (last visited June 3, 2025).

149. Criteo is another supply-side platform that claims to "[m]aximize monetization" by being "the only SSP purpose-built for commerce" that provides "instant access to exclusive demand from 17,000+ brands, retailers, and agencies spending billions annually across Criteo's Commerce Media Platform."[125]

150. Criteo instructs its partner websites like the E! Online website to use "their valuable first-party data to increase yield and revenue."[126] "First-party data refers to data a company collects directly from customers and audiences on its own channels," like the IP addresses of Website users.[127]

151. Indeed, Criteo specifically notes that websites like E! Online can "[c]apture advertiser budgets and generate incremental revenue by opening on-site inventory to programmatic demand [also known as real-time bidding and described in more detail below]."[128]

152. Criteo also provides its own identity graph, known as the "Shopper Graph," that provides "[r]eal-time identity data … ensur[ing] accurate cross-device identification from billions of active shoppers using multiple devices to shop."[129] Specifically, Criteo's Shopper Graph pulls "data from over 720 million active daily shoppers."[130]

153. The upshot of all this is that Criteo enables website owners like E! Online to effectively sell their user inventory to advertisers in a de-anonymized, targeted format. By syncing

---

[125] *Commerce Grid*, CRITEO, https://www.criteo.com/platform/commerce-grid/.

[126] *Commerce Media Platform*, CRITEO, https://www.criteo.com/platform/commerce-media-platform/ (video at 0:37) (last visited June 3, 2025).

[127] Natalia Chronowska, *What is First-Party Data and Hose Does it Benefit Your Marketing*, PIWIK (Jan. 30, 2024), https://piwik.pro/blog/first-party-data-value/.

[128] SHOPPER GRAPH, CRITEO, https://www.criteo.com/technology/shopper-graph/.

[129] *Id*.

[130] *Id*.

its tracker with Defendant's tracker, Criteo facilities this goal, leveraging Defendant's replete database of user profiles (described in more detail below) to de-anonymize and identify website users like users of the E! Online website.

154. Thus, when Criteo offers Website users up for sale to advertisers—as is Criteo's function as a supply-side platform—those users will receive higher bids because they can be better targeted by advertisers as a result of Criteo's synchronization with Defendant. Defendant, in turn, builds on its already expansive database by learning whatever Criteo knows about the user.

3. Magnite (Rubicon)

155. As a final example, as the above screenshot indicates, Defendant syncs its tracker with another tracker installed on the E! Online website that is operated by Magnite, who is also a registered data broker in California.[131] Magnite's tracker is called "Rubicon."

155. Magnite is another supply-side platform that companies like E! Online use "to monetize their content," and "[t]he world's leading agencies and brands trust [Magnite's] platform to access … billions of advertising transactions each month."[132]

156. It is estimated that Magnite collects information on a billion website interactions. "By leveraging [their] platform, [Magnite] believe[s] buyers can reach approximately one billion internet users globally, including through many of the world's largest and most premium sellers."[133]

---

[131] DATA BROKER REGISTRATION FOR MAGNITE INC., https://oag.ca.gov/data-broker/registration/568127.

[132] *iHeartMedia and Magnite Unify Access to Broadcast and Digital Audio, Providing Advertisers with a Direct Path to Premium Inventory*, MAGNITE (Jan. 9, 2024), https://investor.magnite.com/news-releases/news-release-details/iheartmedia-and-magnite-unify-access-broadcast-and-digital audio.

[133] MAGNITE FORM 10-K, at 9 (2016), https://investor.magnite.com/static-files/88921618-9e64-4b6b-9bb1-ef1422015f44.

157. Magnite calls its suite of identity resolution products the Magnite Access Suite.[134]

158. Magnite's suite includes four products: Magnite DMP; Magnite Storefront; Magnite Match; and Magnite Audiences.[135]

159. Magnite DMP helps publishers sell their first-party data. It "enables sellers to seamlessly create, [audience] segment[s]" so they can make their data more valuable to buyers.[136]

160. Magnite Storefront "enables the activation of buyer and seller first-party data on the sell side and facilitates the buying and selling of third-party data–from discovery to activation–across all of Magnite's platforms."[137]

161. Magnite Match is "a cloud-based solution that allows sellers and buyers to establish a match between data sets" so that a publisher's first-party data can be merged and enhanced with other data about the same individual.[138]

162. Magnite Audiences are "cross-publisher segments that Magnite packages to make it easier and more efficient for buyers to reach high value audiences at scale."[139] In other words, Magnite takes a publisher's first-party data and combines it with first-party data from other publishers where the individuals have similar interests based on their web activity, which

---

[134] *Introducing Magnite Access: An Omnichannel Audience, Data and Identity Suite*, MAGNITE (June 15, 2023), https://www.magnite.com/press/introducing-magnite-access-an-omnichannel-audience-data-and-identity-suite/.

[135] *Id*.

[136] *Id*.

[137] *Id*.

[138] *Id*.

[139] *Id*.

"generates a potential new revenue stream for publishers with no additional operational overhead."[140]

163. The upshot of all this is that Magnite enables websites like E! Online to effectively sell their user inventory to advertisers in a de-anonymized, targeted format. By syncing its tracker with Defendant's, Magnite facilities this goal, leveraging Defendant's replete database of user profiles (described in more detail below) to de-anonymize and identify users of websites such as users of the E! Online website.

164. Thus, when Magnite offers Website users up for sale to advertisers—as is Magnite's function as a supply-side platform—those users will receive higher bids because they can be better targeted by advertisers as a result of Magnite's synchronization with Defendant. Defendant, in turn, builds on its already expansive database by learning whatever Magnite knows about the user.

V. PLAINTIFF'S EXPERIENCE

165. Plaintiff Weiler visited multiple websites while in California, including but not limited to the E! Online website.

166. Unbeknownst to Plaintiff Weiler, Defendant's tracker was loaded onto many of the websites she visited. Indeed, according to her CCPA data, Plaintiff Weiler was tracked ***over 45,000 times*** by Defendant between May 2020 and February 2025, including having her e-mail address collected over 21,000 times.

167. Defendant collected at least the following pieces of information from Plaintiff Weiler in real-time and within seconds of Plaintiff's visit to any Partner Website:

(i) E-mail address;

[140] *Id.*

(ii) IP address;

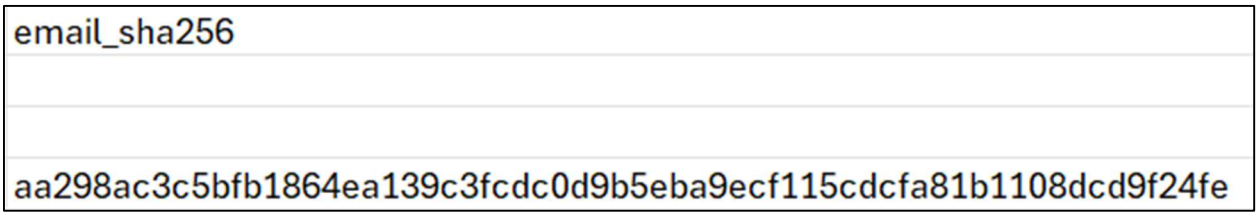
(iii) Device identifying information;

(iv) Data and time of the website visit;

(v) Action category on each website; and

(vi) Information related to the specific product being advertised, which divulges Plaintiff Weiler's interests.

168. Although Defendant "hashed" Plaintiff Weiler's e-mail address, it is still identifiable to her per the comments of the FTC and numerous privacy scholars. Hashing Plaintiff Weiler's e-mail address using SHA-256 (the same algorithm Defendant used) produces the exact same value (see bottom screenshot) as Defendant's encryption (see top screenshot)[141]:



169. Defendant then used this information to compile a comprehensive profile of Plaintiff Weiler and her activity across multiple websites. Defendant could then tie Plaintiff Weiler's activity on other websites to this profile, enabling Plaintiff Weiler to be de-anonymized and surveilled across the Internet.

[141] Plaintiff's e-mail address has been partially redacted to protect her privacy.

170. Defendant then synchronized this profile of Plaintiff Weiler with any of the Partner Pixels deployed on the various Partner Websites. For instance, Defendant synchronized Plaintiff Weiler's profile with PubMatic, Criteo, and Magnite on E! Online.

171. Plaintiff Weiler's profile was then sold to advertisers because of Defendant's synchronization with these Partner Pixels on the Partner Websites.

172. Thus, through Defendant's tracker, Defendant and each of the Partner Pixels and Partner Websites:

(i) identified and de-anonymized Plaintiff by matching Plaintiff to a pre-existing profile maintained by Defendant;

(ii) sold Plaintiff's information to advertisers for hyper-targeted advertising based on the information collected by Defendant the Partner Pixels on each Partner Website and the information contained on the profile of Plaintiff maintained by Defendant;

(iii) actually targeted Plaintiff with advertisements and served advertisements on Plaintiff based on the information collected by Defendant the Partner Pixels on each Partner Website and the information contained on the profile of Plaintiff maintained by Defendant; and

(iv) generated revenue for the Partner Websites from the sale of Plaintiff's information to advertisers—including the profile of Plaintiff maintained by Defendant—thus boosting the value of Defendant's services.

173. Plaintiff Weiler was unaware that Defendant or any Partner Website was installing or using trackers on her browser, aiding in the wiretapping of her communications, de-anonymizing and identifying her, and facilitating the selling and sharing of her personal information to advertisers, other data brokers, or any person or entity doing business with Defendant.

174. Plaintiff Weiler did not provide her prior consent to Defendant or any Partner Website to install or use trackers on her browser, aid in the wiretapping of her communications,

de-anonymizing and identifying her, and facilitating the selling and sharing of her personal information to advertisers, other data brokers, or any person or entity doing business with Defendant. Nor did Defendant obtain a court order to do the same.

175. Plaintiff Weiler has, therefore, had her privacy invaded by Defendant's actions, and Defendant has been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Weiler.

CLASS ALLEGATIONS

176. **Class Definition:** Plaintiff seeks to represent a class of similarly situated individuals defined as follows:

> All persons in the United States whose personal information, communications, or private information, or data derived from their personal information, communications, or private information, was used to create a profile and/or made available for sale or use through Defendant's tracking technology, distributed or sold in the process of delivering advertising on websites, mobile applications, or other digital media, or otherwise.

177. **California Subclass Definition**: Plaintiff seeks to represent an additional subclass of similarly situated individuals defined as follows:

> All persons in the state of California whose personal information, communications, or private information, or data derived from their personal information, communications, or private information, was used to create a profile and/or made available for sale or use through Defendant's tracking technology, mobile applications, or other digital media, or otherwise.

178. Together, the Class and the California Subclass shall be referred to as the "Classes."

179. Excluded from the Classes are Defendant, any affiliate, parent, or subsidiary of any Defendant; any entity in which any Defendant has a controlling interest; any officer director, or employee of any Defendant; any successor or assign of any Defendant; anyone employed by

counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

180. **Numerosity**. Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff currently; however, it is estimated that there are tens or hundreds of millions of individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's records and non-party records, such as those of Defendant's customers and advertising partners.

181. **Typicality**. Plaintiff's claims are typical of the claims of the Classes. Plaintiff, like all Class Members, had their information collected and made available for sale by Defendant using comprehensive user profiles compiled about Plaintiff.

182. **Adequacy**. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Classes. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Classes. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Classes.

183. **Commonality/Predominance**. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

(i) Whether Defendant's acts and practices alleged herein constitute egregious breaches of social norms to the Class and Subclass;

(ii) Whether Defendant acted intentionally in violating Plaintiff's and Class Members' privacy rights under the New York common law;

(iii) Whether Defendant was unjustly enriched because of its violations of Plaintiff's and Class Members' privacy rights; and;

(iv) Whether Plaintiff and California Subclass Members are entitled to damages under CIPA or any other relevant statute.

184. **Superiority**: Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff knows of no special difficulty to that would be encountered by litigating this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

COUNT I
Intrusion Upon Seclusion

185. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

186. Plaintiff brings this claim individually and on behalf of the Class against Defendant.

187. Plaintiff brings this claim pursuant to New York law.

188. To state a claim for intrusion upon seclusion, a plaintiff must allege that "the defendant intentionally intrude[d] upon the plaintiff's solitude, seclusion, private affairs, or private

concerns in a way that would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (1977).

189. Plaintiff and Class Members have an interest in: (i) precluding the dissemination and/or misuse of their sensitive, confidential communications and information; and (ii) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to highly intrusive surveillance at every turn.

190. By conducting such widespread surveillance, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights, as well as intruded upon Plaintiff's and Class Members' seclusion.

191. Plaintiff and Class Members had a reasonable expectation that their communications, identities, personal activities, and other data would remain confidential.

192. Plaintiff and Class Members did not and could not authorize Defendant to intercept data on every aspect of their lives and activities.

193. The conduct described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

(i) Defendant engages in widespread data collection and interception of Plaintiff's and Class Members' internet and app activity, including their communications with websites and apps, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

(ii) Defendant combines the information collected on websites and apps with offline information also gathered on individuals to create the profiles used in the Wunderkind products described herein.

(iii) Defendant creates comprehensive profiles based on this online and offline data, which violates Plaintiff's Class

Members' common law right to privacy and the control of their personal information.

(iv) Defendant sells or discloses these profiles, which contain the improperly collected data about Plaintiff and Class Members, to an unknown number of advertisers for use in the real-time-bidding process, which likewise violates Plaintiff's and Class Members' common law right to privacy and the control of their personal information.

194. Defendant's amassment of electronic information reflecting all aspects of Plaintiff's and Class Members' lives into profiles for future or present use is in and of itself a violation of their right to privacy considering the serious risk these profiles pose to their autonomy.

195. In addition, those profiles are and can be used to further invade Plaintiff's and Class Members' privacy by, for example, allowing third parties to learn intimate details of their lives and target them for advertising, political, and other purposes, as described herein, thereby harming them by selling this data to advertisers and other data brokers without their consent.

196. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims under common law.

COUNT II
Unjust Enrichment

197. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

198. Plaintiff brings this claim individually and on behalf of the California Subclass against Defendant.

199. Plaintiff brings this claim pursuant to California law.

200. Defendant has wrongfully and unlawfully trafficked in the named Plaintiff's and California Subclass Members' personal information and other personal data without their consent for substantial profits.

201. Plaintiff's and California Subclass Members' personal information and data have conferred an economic benefit on Defendant, which was collected and used by Defendant without consent.

202. Defendant has been unjustly enriched at the expense of Plaintiff and California Subclass Members and has unjustly retained the benefits of its unlawful and wrongful conduct.

203. It would be inequitable and unjust for Defendant to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

204. Plaintiff and California Subclass Members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Defendant obtained because of its unlawful and wrongful conduct.

205. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant.

206. Defendant has been unjustly enriched by virtue of its violations of Plaintiff's and California Subclass Members' legally protected rights to privacy as alleged herein, entitling Plaintiff and Class members to restitution of Defendant's enrichment. "[T]he consecrated formula 'at the expense of another' can also mean 'in violation of the other's legally protected rights,' without the need to show that the claimant has suffered a loss." RESTATEMENT (THIRD) OF RESTITUTION § 1, cmt. a.

207. Defendant was aware of the benefit conferred by Plaintiff and California Subclass Members. Indeed, Defendant's data-brokerage products are premised entirely on the sale of such data to third parties. Defendant therefore acted in conscious disregard of the rights of Plaintiff and

California Subclass Members and should be required to disgorge all profit obtained therefrom to deter Defendant and others from committing the same unlawful actions again.

COUNT III
Violation Of The California Invasion of Privacy Act,
Cal. Penal Code § 631(a)

208. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

209. Plaintiff brings this claim individually and on behalf of the California Subclass against Defendant.

210. The California Legislature enacted the CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

211. The California Supreme Court has repeatedly stated the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas*, 38 Cal. 3d at 363 (emphasis added, internal quotations omitted).

212. This restriction is based on the "substantial distinction … between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor*, whether that auditor be a person or mechanical device." *Id.* at 361 (emphasis added). Such "simultaneous dissemination" "denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements." *Id.*; *see also Reporters Committee for Freedom of Press*, 489 U.S. at 763 ("[B]oth

the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

213. Further, "[t]hough written in terms of wiretapping, Section 631(a) applies to Internet communications." *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022). Indeed, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013). This accords with the fact that "the California Supreme Court has [] emphasized that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA." *Javier*, 2022 WL 1744107, at *2. "Thus, when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

214. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

215. To avoid liability under CIPA § 631(a), a defendant must show it had the consent of *all* parties to a communication, and that such consent was procured *prior to* the interception occurring. *See Javier*, 2022 WL 1744107, at *2.

216. The Partner Pixels are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

217. Each entity operating the Partner Pixels is a "separate legal entity that offers [a] 'software-as-a-service' and not merely [a] passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, each entity operating the Partner Pixels has the capability to use the wiretapped information for a purpose other than simply recording the communications and providing the communications to website operators. Accordingly, each entity operating the Partner Pixels was a third party to any communication between Plaintiffs and California Subclass Members, on the one hand, and any of the websites at issue, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

218. At all relevant times, each entity operating the Partner Pixels willfully and without the consent of all parties to the communication, and in an unauthorized manner, read, attempted to read, and learned the contents the electronic communications of Plaintiff and California Subclass Members, on the one hand, and the Partner Websites, on the other, while the electronic

communications were in transit or were being sent from or received at any place within California.

219. At all relevant times, Defendant, by synchronizing with the Partner Pixels, used those intercepted communications, including but not limited to building comprehensive user profiles that are offered for disclosure or sale in real-time bidding to prospective advertisers.

220. At all relevant times, Defendant, by synchronizing with the Partner Pixels, aided and agreed with the Partner Pixels' wiretapping by enabling the Partner Pixels to identify the person (*i.e.*, Plaintiff and California Subclass Members) engaging in communications with the Partner Websites.

221. Plaintiff and California Subclass Members did not provide their prior consent to Defendant's intentional interception, reading, learning, recording, collection, and usage of Plaintiff's and California Subclass Members' electronic communications.

222. The wiretapping of Plaintiff and California Subclass Members occurred in California, where Plaintiff and California Subclass Members accessed the Partner Websites, where Defendant's tracker and the Partner Pixels were loaded on Plaintiff's and California Subclass Members' browsers, and where Defendant and the Partner Pixels routed Plaintiff's and California Subclass Members' electronic communications to Defendant's servers.

223. Pursuant to Cal. Penal Code § 637.2, Plaintiff and California Subclass Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

COUNT IV
Violation Of The California Invasion of Privacy Act, Cal. Penal Code § 638.51(a)

224. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

225. Plaintiff brings this claim individually and on behalf of the members of the proposed California Subclass against Defendant.

226. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

227. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

228. Defendant's tracking technology is a "pen register" because it is a "device or process" that "capture[d]" the "routing, addressing, or signaling information"—the e-mail address, IP address, device identifying information, etc.—from the electronic communications transmitted by Plaintiff's and California Subclass Members' computers or smartphones. Cal. Penal Code § 638.50(b); *see also*, *e.g.*, *Lesh v. Cable News Network, Inc.*, 767 F. Supp. 3d 33, 40-42 (S.D.N.Y. 2025); *Shah v. Fandom, Inc*, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024); *Moody v. C2 Educ. Sys. Inc.* 742 F. Supp. 3d 1072, 1077 (C.D. Cal. 2024); *Greenley v. Kochava, Inc.* 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023).

229. Defendant's tracking technology is also a "pen register" because the information it records is being used to ascertain the identity of "visitors to [the Partner] [W]ebsite[s]," and is thus recording "addressing" information. *Heiting v. FKA Distributing Co.*, 2025 WL 736594, at *3 (C.D. Cal. Feb. 3, 2025); *see also Greenley*, 684 F. Supp. 3d at 1050 ("software that identifies consumers" is a pen register).

230. At all relevant times, the Partner Websites installed Defendant's tracking technology on their respective websites. Defendant then used its tracking technology to identify Plaintiff and California Subclass Members through its collection of "addressing information," set a unique identifier on Plaintiff's and California Subclass Members' browsers, and pervasively track Plaintiff and California Subclass Members across multiple website sessions and multiple websites.

231. Defendant, the Partner Pixels, and the Partner Websites used Defendant's tracking technology to:

(i) identify and de-anonymized Plaintiff and California Subclass Members by matching Plaintiff and California Subclass Members to a pre-existing profile maintained by Defendant;

(ii) sell Plaintiff's and and California Subclass Members' information to advertisers for hyper-targeted advertising based on the information collected by Defendant the Partner Pixels on each Partner Website and the information contained on the profiles of Plaintiff and California Subclass Members maintained by Defendant;

(iii) actually target Plaintiff and California Subclass Members with advertisements and served advertisements on Plaintiff and California Subclass Members based on the information collected by Defendant the Partner Pixels on each Partner Website and the information contained on the profiles of Plaintiff and California Subclass Members maintained by Defendant; and

(iv) generated revenue for the Partner Websites from the sale of Plaintiff's and California Subclass Members' information to advertisers—including the profiles of Plaintiff and California Subclass Members maintained by Defendant—thus boosting the value of Defendant's services.

232. Plaintiff and California Subclass Members did not provide their prior consent to the installation or use of Defendant's tracking technology. Nor did Defendant nor any of the Partner

Pixels nor any of the Partner Websites obtain a court order to install or use Defendant's tracking technology.

233. Pursuant to Cal. Penal Code § 637.2(a), Plaintiff and California Subclass Members have been injured by Defendant's violations of CIPA § 638.51(a), and thus seek statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

COUNT V
Violation Of The Electronic Communications Privacy Act,
18 U.S.C. §§ 2510, *et seq.*

234. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

235. Plaintiff brings this claim individually and on behalf of the Class against Defendant.

236. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

237. The ECPA protects both the sending and the receipt of communications.

238. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

239. The transmission of Plaintiff's website page visits, selections, purchases and persistent identifiers to each website each qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

240. The transmission of this information between Plaintiff and Class members and each website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio,

electromagnetic, photoelectronic, or photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

241. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

242. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

243. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

244. The following instruments constitute "devices" within the meaning of the ECPA:

(i) Any tracking code or SDK used by Defendant; and

(ii) Each Partner Pixel;

245. Plaintiff and Class Members' interactions with each website are electronic communications under the ECPA.

246. As described herein, the Partner Pixels intentionally intercepted and/or endeavored to intercept the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

247. As described herein, Defendant intentionally used and/or endeavored to use the electronic communications of Plaintiff and Class Members illegally intercepted by the Partner Pixels in violation of 18 U.S.C. § 2511(1)(d).

248. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, while knowing or having reason to know that the

information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

249. Defendant intentionally used the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, intrusion upon seclusion, CIPA, and other state wiretapping and data privacy laws, among others.

250. Defendant was not acting under the color of law to intercept Plaintiff's and Class members' wire or electronic communications.

251. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy. Plaintiff and Class members had a reasonable expectation that Defendant would not intercept their communications and sell their data to dozens of parties without their knowledge or consent.

252. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1).

253. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, seek judgment against Defendant, as follows:

(a) For an order certifying the Classes pursuant to Fed. R. Civ. P. 23, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Classes.

(b) For an order finding in favor of Plaintiff and the Classes

on all counts asserted herein;

(c) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

(d) For pre- and post-judgment interest on all amounts awarded; and

(e) For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury on all claims so triable.

Dated: July 16, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta
Yizchak Kopel
Alec M. Leslie
Max S. Roberts
Victoria X. Zhou
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
ykopel@bursor.com
aleslie@bursor.com
mroberts@bursor.com
vzhou@bursor.com

Attorneys for Plaintiff